



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Peter Szor  
Assignee: Symantec Corporation  
Title: RETURN-TO-LIBC ATTACK BLOCKING SYSTEM AND METHOD  
Serial No.: 10/671,202 Filed: September 25, 2003  
Examiner: Unknown Group Art 2131  
Docket No.: SYMC1038 Unit:

Monterey, CA  
January 16, 2004

COMMISSIONER FOR PATENTS  
P.O. BOX 1450  
ALEXANDRIA, VA. 22313-1450

INFORMATION DISCLOSURE STATEMENT UNDER §1.97(b)

Sir:

Pursuant to 37 C.F.R. §§ 1.56, 1.97 and 1.98, Applicant(s) wish to call the following documents (a copy of each is enclosed) to the attention of the Examiner:

**U.S. PATENT DOCUMENTS:**

	DOCUMENT NUMBER	DATE	NAME
1)	5,822,517	10/13/1998	Dotan
2)	6,301,699	10/09/2001	Hollander et al.

**OTHER DOCUMENTS:**

1)	Chien, E. and Szor, P., "Blended Attacks Exploits, Vulnerabilities and Buffer-Overflow Techniques In Computer Viruses", Virus Bulletin Conference, September 2002, Virus Bulletin Ltd., The Pentagon, Abingdon, Oxfordshire, England, pp. 1-36.
2)	Dabak, P., Borate, M. and Phadke, S., "Hooking Windows NT System Services", pp. 1-8 [online]. Retrieved on April 16, 2003. Retrieved from the Internet:<URL:http://www.windowsitlibrary.com/Content/356/06/2.html>.

3)	"How Entercept Protects: System Call Interception", pp. 1-2 [online]. Retrieved on April 16, 2003. Retrieved from the Internet:<URL:http://www.entercept.com/products/technology/kernelmode.asp>. No author provided.
4)	"How Entercept Protects: System Call Interception", pg. 1 [online]. Retrieved on April 16, 2003. Retrieved from the Internet:<URL:http://www.entercept.com/products/technology/interception.asp>. No author provided.
5)	Gordon, J., "Understand ... the Stack (part 1)", pp. 1-8 [online]. Retrieved on August 27, 2003. Retrieved from the Internet:<URL:http://www.jorgon.freemove.co.uk/GoasmHelp/usstack1.htm>
6)	Chew, M. and Song, D., "Mitigating Buffer Overflows by Operating System Randomization", December 2002, 9 pages.
7)	"Entercept Continues to Dominate the Market in Buffer Overflow Protection", pg. 1-2 [online]. Retrieved on August 6, 2003. Retrieved from the Internet:<URL:http://www.entercept.com/news/uspr/07-09-02.asp>. No author provided.

A PTO form 1449 listing these documents is enclosed.

**U.S. PATENT APPLICATIONS (COPIES ENCLOSED):**

	SERIAL NUMBER	FILING DATE	NAME
1)	10/360,341	02/06/03	Szor
2)	10/140,149	05/06/02	Sobel et al.

Citation of the above documents shall not be construed as:

1. an admission that the documents are necessarily prior art with respect to the instant invention;
2. a representation that a search has been made, other than as described above; or
3. an admission that the information cited herein is, or is considered to be, material to patentability as defined in § 1.56(b).

If the USPTO issued a first office action prior to the mailing date of this paper, the Commissioner is hereby authorized to charge any fees required for consideration of



Information Disclosure Statement, and to credit any overpayment of fees to Deposit Account No. 50-0553.

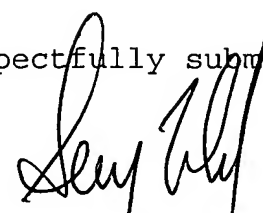
**CERTIFICATE OF MAILING**

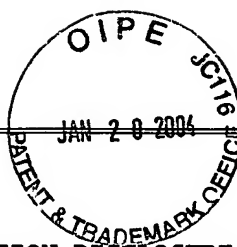
I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA. 22313-1450, on January 16, 2004.

  
Attorney for Applicant(s)

January 16, 2004  
Date of Signature

Respectfully submitted,

  
Serge J. Hodgson  
Attorney for Applicant(s)  
Reg. No. 40,017  
(831) 655-0880



Form PTO-1449

INFORMATION DISCLOSURE CITATION  
IN AN APPLICATION

(Use several sheets if necessary)

Atty Docket No.

SYMC1038

Serial No.

10/671,202

Applicant(s)

Peter Szor

Filing Date

September 25, 2003

Group

2131

## U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
	AA	5,822,517	10/13/1998	Dotan	395	186	
	AB	6,301,699	10/09/2001	Hollander et al.	717	4	
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

## FOREIGN PATENT DOCUMENTS

							Translation	
		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	YES	NO
	AL							
	AM							
	AN							
	AO							
	AP							

## OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

AR	Chien, E. and Szor, P., "Blended Attacks Exploits, Vulnerabilities and Buffer-Overflow Techniques In Computer Viruses", Virus Bulletin Conference, September 2002, Virus Bulletin Ltd., The Pentagon, Abingdon, Oxfordshire, England, pp. 1-36.
AS	Dabak, P., Borate, M. and Phadke, S., "Hooking Windows NT System Services", pp. 1-8 [online]. Retrieved on April 16, 2003. Retrieved from the Internet:<URL:http://www.windowsitlibrary.com/Content/356/06/2.html>.
AT	"How Entercept Protects: System Call Interception", pp. 1-2 [online]. Retrieved on April 16, 2003. Retrieved from the Internet:<URL:http://www.entercept.com/products/technology/kernelmode.asp>. No author provided.

Examiner

Date Considered

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).

Form PTO-1449

JAN 20 2004

Atty Docket No.

Serial No.

SYMC1038

10/671,202

**INFORMATION DISCLOSURE CITATION  
IN AN APPLICATION**

Applicant(s)

Peter Szor

Filing Date

September 25, 2003

Group

2131

(Use several sheets if necessary)

**U.S. PATENT DOCUMENTS**

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

**FOREIGN PATENT DOCUMENTS**

							Translation	
		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	YES	NO
	AL							
	AM							
	AN							
	AO							
	AP							

**OTHER DOCUMENTS** (Including Author, Title, Date, Pertinent Pages, Etc.)

AR	"How Entercept Protects: System Call Interception", pg. 1 [online]. Retrieved on April 16, 2003. Retrieved from the Internet:<URL:http://www.entercept.com/products/technology/interception.asp>. No author provided.
AS	Gordon, J., "Understand ... the Stack (part 1)", pp. 1-8 [online]. Retrieved on August 27, 2003. Retrieved from the Internet:<URL:http://www.jorgon.freeseerve.co.uk/GoasmHelp/usstack1.htm>
AT	Chew, M. and Song, D., "Mitigating Buffer Overflows by Operating System Randomization", December 2002, 9 pages.

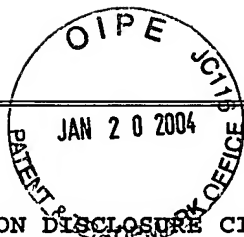
Examiner

Date Considered

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).

Form PTO-1449

JAN 20 2004



**INFORMATION DISCLOSURE CITATION  
IN AN APPLICATION**

(Use several sheets if necessary)

Atty Docket No.

SYMC1038

Serial No.

10/671,202

Applicant(s)

Peter Szor

Filing Date

September 25, 2003

Group

2131

**U.S. PATENT DOCUMENTS**

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

**FOREIGN PATENT DOCUMENTS**

							Translation	
		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	YES	NO
	AL							
	AM							
	AN							
	AO							
	AP							

**OTHER DOCUMENTS** (Including Author, Title, Date, Pertinent Pages, Etc.)

	AR	"Entercept Continues to Dominate the Market in Buffer Overflow Protection", pg. 1-2 [online]. Retrieved on August 6, 2003. Retrieved from the Internet:<URL:http://www.entercept.com/news/uspr/07-09-02.asp>. No author provided.
	AS	
	AT	

Examiner

Date Considered

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).